ABSTRACT OF THE DISCLOSURE

Methods and systems in accordance with the present invention allow users' private keys corresponding to their digital certificates to be stored and archived outside of the control of a Certificate Authority ("CA"). A CA may have a policy that a user's private key must be archived in order to receive a digital certificate upon a registration request from the user. Typically, the CA knows that the user's private key is archived because it implements the archival of the key, for example, on a data recovery manager and associated internal database that the CA controls. Methods and systems in accordance with the present invention allow for the enforcement of such a policy while allowing the archival of the private keys to be outside of the control of the CA by having a data recovery manager supply a digitally signed proof of archival token with a digital certificate request to a CA. The CA is assured that the key has been archived. Methods and systems allow for the data recovery manager and a database of archived keys to be controlled by other entities, including the user or client, for example.

LAW OFFICES
NNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
300 I STREET, N. W.
SHINGTON, DC 20005
202-408-4000